IN THE CLAIMS

Please amend Claims 1, 5, 10-12, 16, 21-23, 25 and 26 as indicated.

Please add new Claims 27-30 as indicated.

Please cancel Claims 2-4, 7, 13-15, 18 and 24 as indicated, without prejudice and without disclaimer of subject matter.

1. (Currently amended) A method for providing automated tracking of security vulnerabilities, comprising:

using a computing device to perform a security vulnerability assessment on a system;

detecting the presence of a security vulnerability in the system; and

responsive to detecting the presence of the security vulnerability:

storing data obtained from the security vulnerability assessment in a security vulnerability database;

determining, using a computer program, a security vulnerability score, the security vulnerability score being a product of a frequency score, a severity score, a criticality score, and a trust score, the frequency score based on a percentage of hosts experiencing the detected security vulnerability in the system and the criticality score based on whether at least one of confidential data and personal data is on the system and whether information on the element is used for aggregation ~~based on a plurality of security vulnerability factors identified by the security vulnerability assessment~~; and

determining a time to fix the security vulnerability detected by the security vulnerability assessment of the system based on the determined security vulnerability score.

2. (Cancelled)

3. (Cancelled)

4. (Cancelled)

5. (Currently amended) The method of claim 1 further comprising entering ~~the~~ an IP address associated with the security vulnerability and a description of the detected security vulnerability in a tracking database.

6. (Previously Presented) The method of claim 1 further comprising determining delinquent security vulnerabilities based upon the determined time to fix the security vulnerability detected by the security vulnerability assessment.

7. (Cancelled)

8. (Previously Presented) The method of claim 6 further comprising re-running a scan profile when notification is received that the security vulnerability has been fixed.

9. (Previously Presented) The method of claim 8 further comprising determining whether the security vulnerability still exists and archiving records associated with the security vulnerability when the security vulnerability does not still exist.

10. (Currently amended) A method for determining a criticality factor for a security vulnerability in a computer system, comprising:

entering in a database security vulnerabilities detected in the computer system during a security vulnerability assessment;

measuring a frequency of occurrence for the detected security vulnerabilities; and

assigning a security vulnerability factor to a detected security vulnerability based upon the frequency of occurrence of the security vulnerability in the system, a criticality of an element in the system, a severity of the security vulnerability within the system, and isolation of the system.

11. (Currently amended) The method of claim 10, wherein the ~~assigning a security vulnerability factor further comprises considering a~~ criticality of an element in the system

~~presenting the security vulnerability and a rating of the severity of the security vulnerability within the system~~ is based on whether at least one of confidential data and personal data is on the system and whether information on the element is used for aggregation.

12. (Currently amended) An apparatus for providing automated tracking of security vulnerabilities, comprising:

a memory for storing program instructions; and

a processor, configured according to the program instructions for:

performing a security vulnerability assessment on a system~~,~~;

detecting the presence of a security vulnerability in the system~~,~~; and

responsive to detecting the presence of the security vulnerability:

storing data obtained from the security vulnerability assessment in a security vulnerability database~~,~~;

determining a security vulnerability score, the security vulnerability score being a product of ~~based on a plurality of security vulnerability factors identified by the security vulnerability assessment~~ a frequency score, a severity score, a criticality score, and a trust score;

the frequency score based on a percentage of hosts experiencing the detected security vulnerability in the system; and

the criticality score based on whether at least one of confidential data and personal data is on the system and whether information on the element is used for aggregation; and

determining a time to fix a security vulnerability detected by the security vulnerability assessment of the system based on the determined security vulnerability score.

13. (Cancelled)

14. (Cancelled)

15. (Cancelled)

16. (Currently amended) The apparatus of claim 12, wherein the processor enters an IP address associated with the security vulnerability and a description of the detected security vulnerability in a tracking database.

17. (Previously Presented) The apparatus of claim 12, wherein the processor identifies delinquent security vulnerabilities based upon the determined time to fix the security vulnerability detected by the security vulnerability assessment.

18. (Cancelled)

19. (Previously Presented) The apparatus of claim 17, wherein the processor re-runs a scan profile when notification is received that the security vulnerability has been fixed.

20. (Previously Presented) The apparatus of claim 19, wherein the processor determines whether the security vulnerability still exists and archives records associated with the security vulnerability when the security vulnerability does not still exist.

21. (Currently amended) An apparatus for determining a criticality factor for a security vulnerability in a computer system, comprising:

a memory for storing program instructions; and

a processor, configured according to the program instructions for entering in a database security vulnerabilities detected in the computer system during a security vulnerability assessment, measuring a frequency of occurrence for the detected security vulnerabilities and assigning a security vulnerability factor to a security vulnerability based upon the frequency of occurrence of the security vulnerability in the system, a criticality of an element in the system, a severity of the security vulnerability within the system, and isolation of the system.

22. (Currently amended) The apparatus of claim 21, wherein the processor considers a criticality of an element in the system ~~presenting the security vulnerability and a rating of the severity of the security vulnerability within the system when assigning a security vulnerability~~

~~factor~~ the criticality based on whether at least one of confidential data and personal data is on the system and whether information on the element is used for aggregation.

23. (Currently amended) An apparatus for providing automated tracking of security vulnerabilities, comprising:

means for storing program instructions; and

means configured according to the program instructions provided by the means for storing for:

performing a security vulnerability assessment on a system~~,~~;

detecting the presence of a security vulnerability in the system~~,~~; and

responsive to detecting the presence of the security vulnerability:

storing data obtained from the security vulnerability assessment in a security vulnerability database~~,~~;

determining a security vulnerability score, the security vulnerability score being a product of ~~based on a plurality of security vulnerability factors identified by the security vulnerability assessment~~ a frequency score, a severity score, a criticality score, and a trust score;

the frequency score based on a percentage of hosts experiencing the detected security vulnerability in the system; and

the criticality score based on whether at least one of confidential data and personal data is on the system and whether information on the element is used for aggregation; and

determining a time to fix a security vulnerability detected by the security vulnerability assessment of the system based on the determined security vulnerability score.

24. (Cancelled)

25. (Currently amended) A program storage device readable by a computer, the program storage device tangibly embodying one or more programs of instructions executable by the computer to perform a method for providing automated tracking of security vulnerabilities, the method comprising:

performing a security vulnerability assessment on a system;

detecting the presence of a security vulnerability in the system; and

responsive to detecting the presence of the security vulnerability:

storing data obtained from the security vulnerability assessment in a vulnerability database;

determining a security vulnerability score based on ~~a plurality of security vulnerability factors identified by the security vulnerability assessment~~ a frequency score, a severity score, a criticality score, and a trust score;

the frequency score based on a percentage of hosts experiencing the detected security vulnerability in the system; and

the criticality score based on whether at least one of confidential data and personal data is on the system and whether information on the element is used for aggregation; and

determining a time to fix a security vulnerability detected by the security vulnerability assessment of the system based on the determined security vulnerability score.

26. (Currently amended) A program storage device readable by a computer, the program storage device tangibly embodying one or more programs of instructions executable by the computer to perform a method for determining a criticality factor for a security vulnerability in a computer system, the method comprising:

entering in a database security vulnerabilities detected in the computer system during a security vulnerability assessment;

measuring a frequency of occurrence for the detected security vulnerabilities; and

assigning a security vulnerability factor to a security vulnerability based upon the frequency of occurrence of the security vulnerability in the system, a criticality of an element in the system, a severity of the security vulnerability within the system, and isolation of the system.

27. (New) The method of claim 1, wherein the severity score is based on whether a host will allow root compromise and whether the security vulnerability is remotely exploitable.

28. (New) The method of claim 1, wherein the trust score is based on whether the system is isolated.

29. (New) The apparatus of claim 12, wherein the severity score is based on whether a host will allow root compromise and whether the security vulnerability is remotely exploitable.

30. (New) The apparatus of claim 12, wherein the trust score is based on whether the system is isolated.